

CLAIMS

1. A method for detecting intrusions in a wireless network, comprising the steps of:
researching and defining normal network behavior with the intent of ascertaining user
5 and temporal patterns;

researching potential sources of information that will lead to the detection and
classification of potentially intrusive events;

establishing a knowledge base of anomalous network activity that will form the
foundation for classifying potentially intrusive events;

10 analyzing and evaluating the knowledge base to create an attack model; and
utilizing the attack model to provide an adaptive response to intrusions in the wireless
network.

2. A method according to claim 1 which further includes augmenting the researching
15 step by collecting real-world information concerning intrusive events and updating the
knowledge base

3. A method according to claim 2 which further includes developing a recovery
model to recover from an intrusion of the wireless network.

20 4. A method according to claim 1 wherein the wireless network is the Tactical
Internet.

5. A method according to claim 1 wherein the wireless network is a Situation
25 Assessment Data Link (SADL).

6. A method according to claim 1 wherein the wireless network is a tactical data link.

7. A method according to claim 1 wherein the tactical data link is a Link-16 type
30 tactical data link and its logical extensions.

8. A method according to claim 1 wherein the tactical data link is a Link-11 type tactical data link and its logical extensions.

9. A method according to claim 1 wherein the tactical data link is a Link-22 type tactical data link

10. A method according to claim 1 wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service.

11. A method according to claim 8 wherein the attack model is utilized to generate signatures of suspicious events.

12. A method according to claim 8 wherein the attack model is utilized to generate recommendations regarding the design of a wireless network.

13. A method for detecting intrusions in a wireless network, comprising the steps of: researching and defining normal network behavior with the intent of ascertaining user and temporal patterns;

researching potential sources of information that will lead to the detection and classification of potentially intrusive events;

augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base;

establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events;

analyzing and evaluating the knowledge base to create an attack model;

utilizing the attack model to provide an adaptive response to intrusions in the wireless network; and

developing a recovery model to recover from an intrusion of the wireless network.

utilizing the IW attack model to provide an adaptive response to intrusions in the RF based tactical data link; and

developing a recovery model to recover from an intrusion of the RF based tactical data link.

5